Exhibit 23

https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics

National Institute of Standards and Technology
U.S. Department of Commerce

Cybersecurity Framework (https://www.nist.gov/cyberframework)

Questions and Answers

Framework Basics

What is the Framework, and what is it designed to accomplish?

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Is my organization required to use the Framework?

No. Use of the Framework is voluntary.

Does it provide a recommended checklist of what all organizations should do?

The Framework is guidance. It should be customized by different sectors and individual organizations to best suit their risks, situations, and needs. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework to achieve positive outcomes will vary. The Framework should not be implemented as an un-customized checklist or a one-size-fits-all approach for all critical infrastructure organizations.

Why should an organization use the Framework?

The Framework will help an organization to better understand, manage, and reduce its cybersecurity risks. It will assist in determining which activities are most important to assure critical operations and service delivery. In turn, that will help to prioritize investments and maximize the impact of each dollar spent on cybersecurity. By providing a common language to address cybersecurity risk management, it is especially helpful in communicating inside and outside the organization. That includes improving communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives of organizations. Organizations also can readily use the Framework to communicate current or desired cybersecurity posture between a buyer or supplier.

When and how was the Framework developed?

Version 1.0 of the Framework was prepared by the National Institute of Standards and Technology (NIST) (https://www.nist.gov/) with extensive private sector input and issued in February 2014. The Framework was developed in response to Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* (https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.whitehouse.gov%2Fthe-press-office%2F2013%2F02%2F12%2Fexecutive-order-improving-critical-infrastructure-cybersecurity&data=02%7C01%7Cnicole.keller%40nist.gov%7C05954e0981dc4918e1b708d5a3d8f334%7C2ab5 27
a93e054655c61dec%7C1%7C0%7C636595074543392193&sdata=FaucXr5iAF8rR04szt7DdATmS80IwdLvvMofg &r

eserved=0), which was issued in 2013. Among other things, the EO directed NIST to work with industry leaders to develop the Framework. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process. NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework. The most recent version, Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) was released on April 16, 2018 following a 45-day public comment period on the second draft of Framework V1.1.

What is the purpose of Executive Order 13636?

Executive Order 13636 outlines responsibilities for Federal Departments and Agencies to aid in *Improving Critical Infrastructure Cybersecurity*. In summary, it assigns these responsibilities and establishes the policy that, "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Who from the private sector helped to develop the Framework?

As the Cybersecurity Framework v1.0 was being developed, thousands of people from diverse parts of industry, academia, and government participated in a host of workshops around the United States. During the course of this public development process, NIST received hundreds of detailed suggestions and comments in response to a request for information (https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fwww.nist.gov%2Fcyberframework%2Frfi-framework-reducing-cyber-risks-critical-infrastructure-2013__%3B!!Nhox7I4E!aVLWQkPUSwIGQBlD6TQ0F9xbOgLgjxDn85Enlj2kfKD1rcN5dojIfOs-3YbCZAayhpVW%24&data=04%7C01%7Cnicole.keller%40nist.gov%7Ce9278a9e58e7432c5c9108d930edd6bf%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637594620347360049%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=3sR2GhmW%2Fs84UVbaG%2BVFuZUXAYuxibnnX1tWqpNaP%2BA%3D&reserved=0) (RFI) and feedback on the public draft version of the Framework (https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fwww.nist.gov%2Fcyberframework%2Finitial-analysis-rfi-2013__%3B!!Nhox7I4E!aVLWQkPUSwIGQBlD6TQ0F9xbOgLgjxDn85Enlj2kfKD1rcN5dojIfOs-3YbCZHrygkBo%24&data=04%7C01%7Cnicole.keller%40nist.gov%7Ce9278a9e58e7432c5c9108d930edd6bf%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637594620347360049%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Whze%2ByKczAuD7lx4DKGTnyYozZmqj741%2BNfp4H%2Frzfg%3D&reserved=0).

NIST routinely engages industry through three primary activities. First, NIST continually and regularly engages in community outreach activities by attending and participating in meetings, events, and roundtable dialogs. Second, NIST solicits direct feedback from industry through requests for information (RFI), requests for comments (RFC), and through the NIST Framework team's email (cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov)). Finally, NIST observes and monitors relevant resources and references published by government, academia, and industry.

Still, many more individuals, organizations and industry stakeholders were directly involved and actively contributed to a series of regular workshops and public comment periods (https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fwww.nist.gov%2Fcyberframework%2Fev 3 B!!Nhox7I4E!aVLWQkPUSwIGQBlD6TQ0F9xbOgLgjxDn85Enlj2kfKD1rcN5dojIfOs-3YbCZFh4DKWt%24&data=04%7C01%7Cnicole.keller%40nist.gov%7Ce9278a9e58e7432c5c9108d930edd6bf% d 8fa4797a93e054655c61dec%7C1%7C0%7C637594620347370005%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMD

AiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=f7xpJMPUOUSyaJ8NR4WiHTBipzvAGy4gm%2B9G3GperyQ%3D&reserved=0) held throughout the process of updating the Framework. This effort culminated in the release of the Cybersecurity Framework Version 1.1.
The Framework is a living document and will continue to be updated, improved and refined as industry provides feedback on implementation.

Why is NIST involved? What is NIST's role in setting cybersecurity standards?

NIST is a federal agency within the United States Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is also responsible for establishing computer- and information technology-related standards and guidelines for federal agencies to use. Many private sector organizations have made widespread use of these standards and guidelines voluntarily for several decades, especially those related to information security.

How can we obtain NIST certification for our Cybersecurity Framework products/implementation?

NIST does not offer certifications or endorsement of Cybersecurity Framework implementations or Cybersecurity Framework-related products or services. NIST shares industry resources (https://www.nist.gov/cyberframework/resources/risk-management-resources) and success stories (https://www.nist.gov/cyberframework/success-stories) that demonstrate real-world application and benefits of the Framework. Sharing your own experiences and successes inspires new use cases and helps users more clearly understand Framework application and implementation. To contribute to these initiatives, contact cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov).

Framework Users

What critical infrastructure does the Framework address?

Critical infrastructure (for the purposes of this Framework) is defined in Presidential Policy Directive (PPD) 21 (http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil) as: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Applicable infrastructure includes utilities providing energy and water as well as sectors covering transportation, financial services, communications, healthcare and public health, food and agriculture, chemical and other facilities, dams, key manufacturers, emergency services and several others.

Does the Framework apply only to critical infrastructure companies?

No. Although it was designed specifically for companies that are part of the U.S. critical infrastructure, many other organizations in the private and public sectors (including federal agencies) are using the Framework. NIST encourages any organization or sector to review and consider the Framework as a helpful tool in managing cybersecurity risks.

Does the Framework benefit organizations that view their cybersecurity programs as already mature?

The Framework can be used by organizations that already have extensive cybersecurity programs, as well as by those just beginning to think about putting cybersecurity management programs in place. The same general approach works for any organization, although the way in which they make use of the Framework will differ depending on their current state and priorities.

How is the Framework being used today?

Organizations are using the Framework in a variety of ways. Many have found it helpful in raising awareness and communicating with stakeholders within their organization, including executive leadership. The Framework is also improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. By mapping the Framework to current cybersecurity management approaches, organizations are learning and showing how they match up with the Framework's standards, guidelines, and best practices. Some parties are using the Framework to reconcile and de-conflict internal policy with legislation, regulation, and industry best practice. The Framework also is being used as a strategic planning tool to assess risks and current practices. The Resources (https://www.nist.gov/cyberframework/framework-resources) and Success Stories (https://www.nist.gov/cyberframework/success-stories) sections provides examples of how various organizations have used the Framework.

Framework Components

What is the Framework Core and how is it used?

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. An example of Framework outcome language is, "physical devices and systems within the organization are inventoried."

The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory.

What are Framework Profiles and how are they used?

A Framework Profile ("Profile") represents the cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important. They can also add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

What are Framework Implementation Tiers and how are they used?

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal regulatory requirements, business/mission objectives, and organizational constraints.

Are the Tiers equivalent to maturity levels?
The Framework Implementation Tiers are not intended to be maturity levels. The Tiers are intended to provide guidance to organizations on the interactions and coordination between cybersecurity risk management and operational risk management. The key tenet of the Tiers is to allow organizations to take stock of their current activities from an organization wide point of view and determine if the current integration of cybersecurity risk management practices is sufficient given their mission, regulatory requirements, and risk appetite. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and would be cost-effective.

What is the relationship between the Framework and NIST Roadmap for the Framework for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/document/csf-roadmap-11-final-042519pdf)**?**
The companion Roadmap was initially released in February 2014 in unison with publication of the Framework version 1.0. The Roadmap discusses NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration. These plans are based on input and feedback received from stakeholders through the Framework development process. This list of high-priority areas is not intended to be exhaustive, but these are important areas identified by NIST and stakeholders that should inform future versions of the Framework. For that reason, the Roadmap will be updated over time in alignment with the most impactful stakeholder cybersecurity activities and the Framework itself. The most recent version can be found here (https://www.nist.gov/document/csf-roadmap-11-final-042519pdf).

Using The Framework

What is the difference between 'using', 'adopting', and 'implementing' the Framework?

In a strict sense, these words are fairly interchangeable. They can mean an organization's use of the Framework as a part of its internal processes. NIST generally refers to "using" the Framework.

Would the Framework have prevented recent highly publicized attacks?

There are no "silver bullets" when it comes to cybersecurity and protecting an organization. For instance, "Zero-day" attacks exploiting previously unknown software vulnerabilities are especially problematic. However, using the Framework to assess and improve management of cybersecurity risks should put organizations in a much better position to identify, protect, detect, respond to, and recover from an attack, minimizing damage and impact.

Does the Framework address the cost and cost-effectiveness of cybersecurity risk management?

Yes. An organization can use the Framework to determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

How does the Framework relate to information sharing?

The Framework provides guidance on how awareness of real and potential threats and vulnerabilities can be used to enhance an organization's cybersecurity program.

Can the Framework help managing risk for assets that are not under my direct management?

Yes. The Functions, Categories, and Subcategories of the Framework Core are expressed as outcomes and are applicable whether you are operating your own assets, or another party is operating assets ce for you. For customized external services such as outsourcing engagements, the Framework ca as the basis for due diligence with the service provider. For packaged services, the Framework used as a set of evaluation criteria for selecting amongst multiple providers.

Should the Framework be applied to and by the entire organization or just to the IT department?

The Framework provides guidance relevant for the entire organization. The full benefits of the Framework will not be realized if only the IT department uses it. The Framework balances comprehensive risk management, with a language that is adaptable to the audience at hand. More specifically, the Function, Category, and Subcategory levels of the Framework correspond well to organizational, mission/business, and IT and operational technology (OT)/industrial control system (ICS) systems level professionals. This enables accurate and meaningful communication, from the C-Suite to individual operating units and with supply chain partners. It can be especially helpful in improving communications and understanding between IT specialists, OT/ICS operators, and senior managers of the organization.

How can the Framework help an organization with external stakeholder communication?

The Framework can be used to communicate with external stakeholders such as suppliers, services providers, and system integrators. More specifically, the Framework Core is a language in which to communicate, while Framework Profiles can be used to express security requirements.

What is the role of senior executives and Board members?

The Framework can be used as an effective communication tool for senior stakeholders (CIO, CEO, Executive Board, etc.), especially as the importance of cybersecurity risk management receives elevated attention in C-suites and Board rooms. The Functions inside the Framework Core offer a high level view of cybersecurity activities and outcomes that could be used to provide context to senior stakeholders beyond current headlines in the cybersecurity community.

How can organizations measure the effectiveness of the Framework?

Framework effectiveness depends upon each organization's goal and approach in its use. Is the organization seeking an overall assessment of cybersecurity-related risks, policies, and processes? Is it seeking a specific outcome such as better management of cybersecurity with its suppliers or greater confidence in its assurances to customers? Effectiveness measures vary per use case and circumstance. Accordingly, the Framework leaves specific measurements to the user's discretion. Individual entities may develop quantitative metrics for use within that organization or its business partners, but there is no specific model recommended for measuring effectiveness of use.

How long does it take to implement the Framework?

Each organization's cybersecurity resources, capabilities, and needs are different. So the time to implement the Framework will vary among organizations, ranging from as short as a few weeks to several years. The Framework Core's hierarchical design enables organizations to apportion steps between current state and desired state in a way that is appropriate to their resources, capabilities, and needs. This allows organizations to develop a realistic action plan to achieve Framework outcomes in a reasonable time frame, and then build upon that success in subsequent activities.

Does the Framework require using any specific technologies or products?

No. It has been designed to be flexible enough so that users can make choices among products and services available in the marketplace. It encourages technological innovation by aiming for strong cybersecurity protection without being tied to specific offerings or current technology.

Is a conformity assessment program being planned?

NIST has no plans to develop a conformity assessment program. NIST encourages the private determine its conformity needs, and then develop appropriate conformity assessment progran s able to discuss conformity assessment-related topics with interested parties.

Will my organization be regulated against gaps between my current regulation and Framework?

The Framework was created with the current regulatory environment in mind, and does not replace or augment any existing laws or regulations. The Framework leverages industry best practices and methods for cybersecurity risk management, which are often used in regulation.

Is there a way to find out how organizations have used the Framework, and is there a place to get guidance that would help others?

Early users of the Framework are beginning to produce case studies, implementation guides, and other resources. These resources are starting to be available through trade and professional associations. NIST is also listing those items at the Framework website on the Framework Resources (https://www.nist.gov/cyberframework/framework-resources-0) and Success Stories (https://www.nist.gov/cyberframework/success-stories) pages.

What if Framework guidance or tools do not seem to exist for my sector or community?

The Framework is designed to be applicable to any organization in any part of the critical infrastructure or broader economy. Applications from one sector may work equally well in others. It is expected that many organizations face the same kinds of challenges. There are published case studies and guidance that can be leveraged, even if they are from different sectors or communities. Organizations can encourage associations to produce sector-specific Framework mappings and guidance and organize communities of interest. You may also find value in coordinating within your organization or with others in your sector or community.

Why did NIST create the Perspectives web pages?

The Perspectives (https://www.nist.gov/cyberframework/perspectives) web pages are meant to inform people's decision to use the Framework. The pages contain meaningful quotes that describe why the Framework is important or recommend its use. Survey information that indicates usage is also provided.

What are Success Stories?

NIST is publishing brief Success Stories (https://www.nist.gov/cyberframework/success-stories) explaining how diverse organizations use the Framework to improve their cybersecurity risk management. Success stories are prepared by organizations using the Framework following a template (https://www.nist.gov/document/csf-success-story-template-updated-1-17-2020) and guidance provided by NIST.

How is cyber resilience reflected in the Cybersecurity Framework?

NIST Special Publication (SP) 800-160, Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy secure systems (https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final), defines cyber resiliency as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source. Cyber resiliency has a strong relationship to cybersecurity but, like privacy, represents a distinct problem domain and solution space. Cyber resiliency supports mission assurance, for missions which depend on IT and OT systems, in a contested environment. The Cybersecurity Framework specifically addresses cyber resiliency through the ID.BE-5 and PR.PT-5 subcategories, and through those within the Recovery function. Other Cybersecurity Framework subcategories may help organizations determine whether their curr
adequately supports cyber resiliency, whether additional elements are necessary, and how to c
if any. Many organizations find that they need to ensure that the target state includes an effect
combination of fault-tolerance, adversity-tolerance, and graceful degradation in relation to the mission

goals. The Cybersecurity Framework supports high-level organizational discussions; additional and more detailed recommendations for cyber resiliency may be found in various cyber resiliency models/frameworks and in guidance such as in SP 800-160 Vol. 2.

What is the Cybersecurity Framework's role in supporting an organization's compliance requirements?

The common structure and language of the Cybersecurity Framework is useful for organizing and expressing compliance with an organization's requirements. The Framework provides a flexible, risk-based approach to help organizations manage cybersecurity risks and achieve its cybersecurity objectives. Those objectives may be informed by and derived from an organization's own cybersecurity requirements, as well as requirements from sectors, applicable laws, and rules and regulations.

How do I use the Cybersecurity Framework to prioritize cybersecurity activities?

The Framework can help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. For example, Framework Profiles can be used to describe the current state and/or the desired target state of specific cybersecurity activities. Current Profiles indicate the cybersecurity outcomes that are currently being achieved, while Target Profiles indicate the outcomes needed to achieve the desired cybersecurity risk management goals. Comparing these Profiles may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory of the Framework Core can aid in setting priorities considering the organization's business needs and its risk management processes.

The Framework Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which can also aid in prioritizing and achieving cybersecurity objectives. Tiers help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices.

With an understanding of cybersecurity risk tolerance, organizations can prioritize cybersecurity activities, enabling them to make more informed decisions about cybersecurity expenditures. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. Risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

Small Business Use

Does the Framework apply to small businesses?

Yes. The approach was developed for use by organizations that span the largest to the smallest organizations.

Will NIST provide guidance for small businesses? Is there a starter kit or guide for organizations just getting started with cybersecurity?

NIST has a long-standing and on-going effort supporting small business cybersecurity. This is accomplished by providing guidance through websites, publications, meetings, and events. This includes a Small Business Cybersecurity Corner (https://www.nist.gov/itl/smallbusinesscyber) website that puts a variety of government and other cybersecurity resources for small businesses in one site. That includes the Federal Trade Commission's information about how small businesses can make use of the Cybersecurity Framework.

NIST coordinates its small business activities with the Small Business Administration (https://www.sba.gov/managing-business/cybersecurity), the National Initiative For Cybersecurity Education (NICE) (https://www.nist.gov/itl/applied-cybersecurity/nice), National Cyber Security Alliance (https://staysafeonline.org/cybersecure-business/), the Department of Homeland Security (https://www.us-cert.gov/ncas/tips), the FTC (https://www.ftc.gov/tips-advice/business-center/small-businesses), and others.

Small businesses also may find Small Business Information Security: The Fundamentals (https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final) (NISTIR 7621 Rev. 1) a valuable publication for understanding important cybersecurity activities. It is recommended as a starter kit for small businesses. The publication works in coordination with the Framework, because it is organized according to Framework Functions.

U.S. Federal Agency Use

Are U.S. federal agencies required to apply the Framework to federal information systems?

Yes. On May 11, 2017, the President issued an *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal). In part, the order states that "Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order" and "describe the agency's action plan to implement the Framework."

Can U.S. Federal agencies apply the Framework to Federal information systems?

Yes. The Framework can help agencies to integrate existing risk management and compliance efforts and structure consistent communication, both across teams and with leadership. It can be valuable in managing federal information and information systems according to the Risk Management Framework (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf) (RMF), implementing security controls detailed in SP 800-53 r5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final), and using the methodology outlined in SP 800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf).

How is NIST integrating the Cybersecurity Framework into the cybersecurity risk management practices of federal agencies?

NIST is updating its suite of cybersecurity and privacy risk management publications (*e.g.* SP 800-37 – *Guide for Applying the Risk Management Framework to Federal Information Systems*) to provide additional guidance on how to integrate implementation of the Framework. Similarly, the larger suite of NIST security and privacy risk management publications will be updated in consideration of NIST IR 8170 feedback and general Framework value.

Why did NIST author Interagency Publication 8170?

Federal agencies are now required by a May 2017, Executive Order (https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/) to a
Framework to federal information systems. (See Section 1(c)(ii) of the Order.) The Framework
agencies to integrate existing risk management and compliance efforts and to structure consis

communication, both across teams and with leadership. NIST developed NIST Interagency Report (IR) 8170: Approaches for Federal Agencies to Use the Cybersecurity Framework (https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf) to provide federal agencies with guidance on how the Cybersecurity Framework can help agencies to complement those existing risk management practices and improve their cybersecurity risk management programs. The draft report summarizes eight private sector uses of the Framework, which may also be useful for federal agencies.

What is the relationship between the Framework and NIST's Managing Information Security Risk: Organization, Mission, and Information System View (Special Publication 800-39)?

The Framework uses risk management processes to enable organizations to inform and prioritize cybersecurity decisions. It can be adapted to provide a flexible, risk-based implementation that can be used with a broad array of risk management processes, including, for example, SP 800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf). SP 800-39 describes the risk management process employed by federal organizations, and optionally employed by private sector organizations. The process is composed of four distinct steps: Frame, Assess, Respond, and Monitor. SP 800-39 further enumerates three distinct organizational Tiers at the Organizational, Mission/Business, and System level, and risk management roles and responsibilities within those Tiers. Organizations using the Framework may leverage SP 800-39 to implement the high-level risk management concepts outlined in the Framework. Within the SP 800-39 process, the Cybersecurity Framework provides a language for communicating and organizing. Further, Framework Profiles can be used to express risk disposition, capture risk assessment information, analyze gaps, and organize remediation.

What is the relationship between the Framework and NIST's Guide for Applying the Risk Management Framework to Federal Information Systems (SP 800-37)?

Federal agencies manage information and information systems according to the Federal Information Security Management Act of 2002 (http://csrc.nist.gov/drivers/documents/FISMA-final.pdf) *(FISMA)* and a suite of related standards and guidelines. Perhaps the most central FISMA guideline is NIST Special Publication (SP) 800-37 Risk Management Framework for Federal Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf), which details the Risk Management Framework (RMF). The RMF six-step process provides a method of coordinating the interrelated FISMA standards and guidelines to ensure systems are provisioned, assessed, and managed with appropriate security including incorporation of key Cybersecurity Framework, privacy risk management, and systems security engineering concepts (https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final). NIST held an open workshop for additional stakeholder engagement and feedback on the discussion draft of the Risk Management Framework, including its consideration of the Cybersecurity Framework.

NIST Interagency Report (IR) 8170: Approaches for Federal Agencies to Use the Cybersecurity Framework (https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf) identifies three possible uses of the Cybersecurity Framework in support of the RMF processes: “Maintain a Comprehensive Understanding of Cybersecurity Risk,” “Report Cybersecurity Risks,” and “Inform the Tailoring Process.” The CSF Core can help agencies to better-organize the risks they have accepted and the risk they are working to remediate across all systems, use the reporting structure that aligns to SP 800-53 r5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final), and enables agencies to reconcile mission objectives with the structure of the Core.

For more information, please see the CSF's Risk Management Framework page (https://www.nist.gov/node/1611271).

What type of NIST publication is The Framework for Improving Critical Infrastru Cybersecurity?

Given the broad applicability of the Cybersecurity Framework and the requirement for neutral authorities for what is primarily a voluntary guidance, the document was published as, and remains, a white paper. It is not an Interagency Report, Special Publication, or Federal Information Processing Standard.

How is NIST integrating the Cybersecurity Framework into the cybersecurity risk management practices of federal agencies?

NIST is updating its suite of cybersecurity and privacy risk management publications (e.g. SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf)) to provide additional guidance on how to integrate implementation of the Framework. Similarly, the larger suite of NIST security and privacy risk management publications will be updated based on Executive Order 13800 (https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure) and feedback received in the development of NIST Interagency Report (IR) 8170: Approaches for Federal Agencies to Use the Cybersecurity Framework (https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf).

Relationship Between the Framework and Other Approaches and Initiatives

What is the relationship between the Cybersecurity Framework and the NICE Cybersecurity Workforce Framework?

Workforce plays a critical role in managing cybersecurity, and many of the Cybersecurity Framework outcomes are focused on people and the processes those people perform. While some outcomes speak directly about the workforce itself (e.g., roles, communications, training), each of the Core subcategory outcomes is accomplished as a task (or set of tasks) by someone in one or more work roles. One could easily append the phrase "by skilled, knowledgeable, and trained personnel" to any one of the 108 subcategory outcomes. From this perspective, the Cybersecurity Framework provides the "what" and the NICE Framework provides the "by whom."

While the Cybersecurity Framework and the NICE Framework were developed separately, each complements the other by describing a hierarchical approach to achieving cybersecurity goals.

The Cybersecurity Workforce Framework was developed and is maintained by the National Initiative for Cybersecurity Education (NICE), a partnership among government, academia, and the private sector with a mission to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. Where the Cybersecurity Framework provides a model to help identify and prioritize cybersecurity actions, the NICE Framework (NIST Special Publication 800-181 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf)) describes a detailed set of work roles, tasks, and knowledge, skills, and abilities (KSAs) for performing those actions.

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/document/csf-roadmap-11-final-042519pdf), a companion document to the Cybersecurity Framework, reinforces the need for a skilled cybersecurity workforce. It recognizes that, as cybersecurity threat and technology environments evolve, the workforce must adapt in turn. The NICE program supports this vision and includes a strategic goal of helping employers recruit, hire, develop, and retain cybersecurity talent. One objective within this strategic goal is to publish and raise awareness of the NICE Framework and encourage adoption. Adoption, in this case, means that the NICE Framework is used as a reference resource for actions related to cybersecurity workforce, training, and education.

What is the relationship between the Cybersecurity Framework and the NIST Privacy Framework?

NIST modeled the development of the Privacy Framework (https://www.nist.gov/privacy-framework
successful, open, transparent, and collaborative approach used to develop the Cybersecurity F

(https://www.nist.gov/cyberframework/framework). While good cybersecurity practices help manage privacy risk by protecting information, those cybersecurity measures alone are not sufficient to address the full scope of privacy risks that also arise from how organizations collect, store, use, and share this information to meet their mission or business objective, as well as how individuals interact with products and services.

During the development process, numerous stakeholders requested alignment with the structure of the Cybersecurity Framework so the two frameworks could more easily be used together. In response to this feedback, the Privacy Framework follows the structure of the Cybersecurity Framework, composed of three parts: the Core, Profiles, and Implementation Tiers.

This structure enables a risk- and outcome-based approach that has contributed to the success of the Cybersecurity Framework as an accessible communication tool. In addition, the alignment aims to reduce complexity for organizations that already use the Cybersecurity Framework.

Details about how the Cybersecurity Framework and Privacy Framework functions align and intersect can be found in the Privacy Framework FAQs (https://www.nist.gov/privacy-framework/frequently-asked-questions).

What is the relationship between the Framework and the DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program?

EO 13636 directed the National Institute of Standards and Technology to work with industry to develop a framework for reducing cybersecurity risks. The EO also charged the Department of Homeland Security with developing a voluntary program to promote use of the Framework and help critical infrastructure organizations improve their cybersecurity. In February 2014, DHS launched the Critical Infrastructure Cyber Community (C^3, pronounced "C-Cubed") Voluntary Program. The C^3 Voluntary Program helps align critical infrastructure owners and operators with existing resources to assist in their efforts to use the Framework and manage their cybersecurity risks. More information about the C^3 Voluntary Program may be found on the DHS Web site (http://www.us-cert.gov/ccubedvp).

What is the relationship between the Framework and the DHS Cyber Resilience Review?

A description of the relationship between the DHS Cyber Resilience Review (CRR) and the Cybersecurity Framework can be found at the DHS Web site (https://www.us-cert.gov/ccubedvp/self-service-crr#relationship).

Is the Framework being aligned with international cybersecurity initiatives and standards?

While the Framework was born through U.S. policy, it is not a "U.S. only" Framework. Private sector stakeholders made it clear from the outset that global alignment is important to avoid confusion and duplication of effort, or even conflicting expectations in the global business environment. These needs have been reiterated by multi-national organizations. The importance of international standards organizations and trade associations for acceptance of the Framework's approach has been widely recognized. Some countries and international entities are adopting approaches that are compatible with the framework established by NIST, and others are considering doing the same. The Framework has been translated into several other languages. NIST has been holding regular discussions with many nations and regions, and making noteworthy internationalization progress. NIST is actively engaged with international standards-developing organizations to promote adoption of approaches consistent with the Framework.

What is the relationship between the Framework and NIST's Cyber-Physical Systems (CPS) Framework?

The Cybersecurity Framework provides the underlying cybersecurity risk management princip
support the new Cyber-Physical Systems (CPS) Framework. The CPS Framework document is

to help manufacturers create new CPS that can work seamlessly with other smart systems that bridge the physical and computational worlds.

The CPS Framework (https://pages.nist.gov/cpspwg/) includes a structure and analysis methodology for CPS. The goal of the CPS Framework is to develop a shared understanding of CPS, its foundational concepts and unique dimensions, promoting progress through the exchange of ideas and integration of research across sectors and to support development of CPS with new functionalities.

What is the relationships between Internet of Things (IoT) and the Framework? Do we need an 'IoT Framework?'

The Cybersecurity Framework is applicable to many different technologies, including Internet of Things (IoT) technologies. Developing separate frameworks of cybersecurity outcomes specific to IoT might risk losing a critical mass of users aligning their cybersecurity outcomes to the Cybersecurity Framework. To retain that alignment, NIST recommends continued evaluation and evolution of the Cybersecurity Framework to make it even more meaningful to IoT technologies. NIST welcomes observations from all parties regarding the Cybersecurity Framework's relevance to IoT, and will vet those observations with the NIST Cybersecurity for IoT Program (https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program).

What is the relationship between the Framework and the Baldrige Cybersecurity Excellence Builder?

The Baldrige Cybersecurity Excellence Builder (https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative#bceb) blends the systems perspective and business practices of the Baldrige Excellence Framework with the concepts of the Cybersecurity Framework. More specifically, the Cybersecurity Framework aligns organizational objectives, strategy, and policy landscapes into a cohesive cybersecurity program that easily integrates with organizational enterprise risk governance. These Cybersecurity Framework objectives are significantly advanced by the addition of the time-tested and trusted systems perspective and business practices of the Baldrige Excellence Framework. The builder responds to requests from many organizations to provide a way for them to measure how effectively they are managing cybersecurity risk.

What is the relationship between threat and cybersecurity frameworks?

Threat frameworks are particularly helpful understanding current or potential attack lifecycle stages of an adversary against a given system, infrastructure, service, or organization. They characterize malicious cyber activity, and possibly related factors such as motive or intent, in varying degrees of detail. Threat frameworks stand in contrast to the controls of cybersecurity frameworks that provide safeguards against many risks, including the risk that adversaries may attack a given system, infrastructure, service, or organization. While NIST has not promulgated or adopted a specific threat framework, we advocate the use of both types of frameworks as tools to make risk decisions and evaluate the safeguards thereof. In particular, threat frameworks may provide insights into which safeguards are more important at this instance in time, given a specific threat circumstance. As circumstances change and evolve, threat frameworks provide the basis for re-evaluating and refining risk decisions and safeguards using a cybersecurity framework. A threat framework can standardize or normalize data collected within an organization or shared between them by providing a common ontology and lexicon.

Example threat frameworks include the U.S. Office of the Director of National Intelligence (ODNI) Cyber Threat Framework (https://www.dni.gov/index.php/cyber-threat-framework) (CTF), Lockheed Martin's Cyber Kill Chain® (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html), and the Mitre Adversarial Tactics, Techniques & Common Knowledge (https://attack.mitre.org/wiki/Main_Page) (ATT&CK) model. Each threat framework depicts a progression of attack steps where successive steps build on the last
the highest level of the model, the ODNI CTF relays this information using four Stages – Prepa
Engagement, Presence, and Consequence. These Stages are de-composed into a hierarchy of (
Actions, and Indicators at three increasingly-detailed levels of the CTF, empowering professionals of

varying levels of understanding to participate in identifying, assessing, managing threats. This property of CTF, enabled by the de-composition and re-composition of the CTF structure, is very similar to the Functions, Categories, and Subcategories of the Cybersecurity Framework. In its simplest form, the five Functions of Cybersecurity Framework – Identify, Protect, Detect, Respond, and Recover – empower professionals of many disciplines to participate in identifying, assessing, and managing security controls. It is recommended that organizations use a combination of cyber threat frameworks, such as the ODNI Cyber Threat Framework, and cybersecurity frameworks, such as the Cybersecurity Framework, to make risk decisions.

What is the difference between a translation and adaptation of the Framework?

A translation is considered a direct, literal translation of the language of Version 1.0 or 1.1 of the Framework. No content or language is altered in a translation. Current translations can be found on the International Resources (https://www.nist.gov/cyberframework/international-resources) page.

An adaptation is considered a version of the Framework that substantially references language and content from Version 1.0 or 1.1 but incorporates new, original content. An adaptation can be in any language. Current adaptations can be found on the International Resources (https://www.nist.gov/cyberframework/international-resources) page.

What is the relationship between the PNT Cybersecurity Profile and the Cybersecurity Framework?

The Positioning, Navigation, and Timing (PNT) Profile (https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf) was created using the NIST Cybersecurity Framework and can be applied as part of a risk management program to help organizations manage risks to systems, networks, and assets that use PNT services. The PNT Profile is broadly applicable and can serve as a foundation for the development of sector-specific guidance. It provides a flexible framework for users to manage risks when forming and using PNT signals and data, which are susceptible to disruptions and manipulations that can be natural, manufactured, intentional, or unintentional.

The PNT Profile is intended to be implemented within the larger context of an organization that is developing and executing its own cybersecurity program. It is best implemented if a cybersecurity program is in place at the organizational level. However, that does not preclude any organization from implementing the PNT Profile even if a cybersecurity program is not yet in place.

The Cybersecurity Framework Core Functions and guidance in the PNT Profile address the generic needs of PNT users in critical infrastructure that depend on PNT services to meet their business objectives. In order to support a risk-based, practical, and effective approach to the responsible use of PNT, organizations can select, tailor, and augment the security controls defined in PNT references. For detailed information about how the Cybersecurity Framework was used to develop the PNT Profile, see section 4 of the PNT Profile.

Updates to the Cybersecurity Framework

How often will NIST update the Framework?

The Framework will be refined, improved, and evolved over time to keep pace with technology and threat trends, integrate lessons learned, and establish best practice as common practice. Decisions about the timing of updates will be made based on user experiences, technological advances, and standards innovations. The Framework update process integrates the NIST Cybersecurity Risk Managem Conference into a public-private dialog that asks stakeholders every three years:

For more information, see: https://www.nist.gov/cyberframework/online-learning/update-process (https://www.nist.gov/cyberframework/online-learning/update-process)

Is it an appropriate time for an update, and if so

What would you like to see in that update?

How did NIST process the V1.1 update?

Framework stakeholders provided initial feedback to NIST through: a December 2015 Request for Information (https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity) lessons learned from Framework use, shared resources from industry partners, and an April 2016 Cybersecurity Framework workshop (https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016). When Version 1.1 Draft 1 was issued on January 10, 2017, NIST solicited comments and held a workshop in May 2017 (https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017) to review and discuss those and other comments. NIST also considered feedback received through meetings and events since the release of Framework Version 1.0 (https://www.nist.gov/document/cybersecurity-framework-021214pdf), as well as advances made in areas identified in the Roadmap (https://www.nist.gov/document/csf-roadmap-11-final-042519pdf) issued in February 2014 when the Framework was initially published. Incorporating feedback received from the May 2017 workshop in addition to the previous workshops and January 10, 2017 Request for Comments (https://www.nist.gov/document/rfc2-response-initial-analysis-20170515pdf), NIST updated the Framework V1.1 Draft. On December 5, 2017 NIST released Framework V1.1 Draft 2 (https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework) and an additional round of comments were received through a 45-day Request for Comment period. NIST then released Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) on April 16, 2018.

How did NIST determine features for this update?

Framework stakeholders provided initial feedback to NIST through: a December 2015 Request for Information (https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity), lessons learned from Framework use, shared resources from industry partners, and an April 2016 Cybersecurity Framework workshop (https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016). When Version 1.1 Draft 1 was issued on January 10, 2017, NIST solicited comments and held a workshop in May 2017 to review and discuss those and other comments. NIST also considered feedback received through meetings and events since the release of Framework Version 1.0 (https://www.nist.gov/document/cybersecurity-framework-021214pdf), as well as advances made in areas identified in the Roadmap (https://www.nist.gov/document/csf-roadmap-11-final-042519pdf) issued in February 2014 when the Framework was initially published.

What changes are included in Framework V1.1?

The changes made for Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) include:

- Declares applicability of the Framework for "technology," which is minimally composed of information technology, operational technology, cyber-physical systems, and Internet of Things,
- Enhances guidance for applying the Framework to supply chain risk management,
- Summarizes the relevance and utility of Framework measurement for organizational self-assessment,
- Better accounts for authorization, authentication, and identity proofing, and
- Administratively updates the Informative References.

For additional information on the Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) updates, a Cybersecurity Framework V1.1 Overview webcast (https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview) is available.

Were there changes proposed to the Framework in light of progress made in areas identified in the 2014 Roadmap?

Yes. The most notable changes are related to Supply Chain Risk Management, where multiple provisions have been added, including a new category in the Framework Core and a new property within Implementation Tiers. Additional provisions related to identity management and access control have been included in V1.1. Also, statements about federal agencies and the Framework are included in V1.1. Informative References also have been updated, reflecting the advancement of standards and guidelines by private and public-sector organizations.

What does this mean for organizations that already have incorporated the current Framework?

Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) is intended to be fully compatible with V1.0. NIST recommends that organizations incorporate the additional content and functionality of V1.1 based on the needs of the individual organization.

Should I use V1.0 or V1.1?

Framework V1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective. As with Version 1.0, users are encouraged to customize the Framework to maximize individual organizational value.

What assistance will NIST provide to organizations that choose to incorporate the additional content and functionality of the new version of the Framework?

NIST will continue to educate organizations through both NIST-hosted and other events. NIST will regularly update its web-based FAQs (https://www.nist.gov/cyberframework/frequently-asked-questions), Presentations (https://www.nist.gov/cyberframework/events-and-presentations), Resources (https://www.nist.gov/cyberframework/framework-resources-0), Online Learning (https://www.nist.gov/cyberframework/online-learning), and Success Stories (https://www.nist.gov/cyberframework/success-stories) pages which offer information about how organizations are using or citing the Framework. NIST also will continue to respond to questions it receives at: cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov).

Informative References

What are Informative References?

Informative References show relationships between any number and combination of organizational concepts (e.g., Functions, Categories, Subcategories, Controls, Control Enhancements) of the Focal Document and specific sections, sentences, or phrases of Reference Documents. The discrete concepts of the Focal Document are called Focal Document elements, and the specific sections, sentences, or phrases of the Reference Document are called Reference Document elements.

What is the National Online Informative References (OLIR) Program?

The National Online Informative References (OLIR) Program is a NIST effort to facilitate subject matter experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their cybersecurity, privacy, and workforce documents and elements of other cybersecurity, privacy, and workforce documents like the Cybersecurity Framework. Informative references were introduced in The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as simple prose mappings that only noted a relationship existed, but not the nature of the relationship. In addition, informative references could not be readily updated to reflect changes in the relationships as they were part of the Cybersecurity Framework document itself.

At this stage of the OLIR Program evolution, the initial focus has been on relationships to cybersecurity and privacy documents. The OLIRs are in a simple standard format defined by NISTIR 8278A (Formerly NISTIR 8204), National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers (https://csrc.nist.gov/publications/detail/nistir/8278a/final) and they are searchable in a centralized repository. By following this approach, cybersecurity practitioners can use the OLIR Program as a mechanism for communicating with owners and users of other cybersecurity documents. You can find the catalog at: https://csrc.nist.gov/projects/olir/informative-reference-catalog (https://csrc.nist.gov/projects/olir/informative-reference-catalog).

Refer to NIST Interagency or Internal Reports (IRs) NISTIR 8278 (https://csrc.nist.gov/publications/detail/nistir/8278/final) and NISTIR 8278A (https://csrc.nist.gov/publications/detail/nistir/8278a/final) which detail the OLIR program. The NISTIR 8278 (https://csrc.nist.gov/publications/detail/nistir/8278/final) focuses on the OLIR program overview and uses while the NISTIR 8278A (https://csrc.nist.gov/publications/detail/nistir/8278a/final) provides submission guidance for OLIR developers.

The NIST OLIR program welcomes new submissions. For those interested in developing informative references, NIST is happy to aid in this process and can be contacted at olir@nist.gov (https://www.nist.govmailto:olir@nist.gov).

Why were Online Informative References necessary?

Historically, Informative References appear in many NIST documents. A subset of related Informative References were published in those documents to maintain readability. The OLIR program scales to accommodate a greater number of Informative References and provides a more agile support model to account for the varying update cycles of all Reference documents. The OLIR program allows for the cybersecurity and privacy community to keep information current on relationship assertions from Informative References to cybersecurity and privacy documents. The OLIR program also provides a more robust method to clearly define those relationship assertions.

Where can I comment, and provide feedback about the Online Informative Reference Program?

NIST welcomes feedback to olir@nist.gov (https://www.nist.govmailto:olir@nist.gov).

What is the difference between an Informative Reference and a Reference Document?

A Reference Document is a cybersecurity or privacy document that is being related to a focal document (e.g., Cybersecurity Framework version 1.1, Privacy Framework version 1.0, and NIST SP 800-53 Rev. 4). An Informative Reference is a separate work product that shows multiple relationship assertions between specific Reference document elements and focal document elements.

Are Informative References publicly available?

Yes. Once the submitting organization has refined the Informative Reference to NIST's specifi d submitted it for public review, it becomes publicly available through a link on the OLIR Inforn

Reference Catalog (https://csrc.nist.gov/Projects/Cybersecurity-Framework/Informative-Reference-Catalog) and is hosted on the Internet by the submitting organization.

Who can author and submit Informative References?

Anyone can author and submit Informative References. The NIST process for accepting, vetting, and linking to these stakeholder submissions is described in NISTIR 8278A (Formerly NISTIR 8204), National Cybersecurity Online Informative References (OLIR) Program: Submission Guidance for OLIR developers (https://csrc.nist.gov/publications/detail/nistir/8278a/final). Questions and draft Informative Reference documents may be directed to olir@nist.gov (https://www.nist.govmailto:olir@nist.gov).

If more than one Informative Reference is submitted for a single Reference Document, which one should I use?

The OLIR site is meant to be a community catalog. However, the Informative References themselves come with no guarantees or endorsements from NIST. Therefore, it is incumbent on the consumer of Informative References to do their due diligence when making business/security decisions for implementation. The implementing party may give preference to a particular Informative Reference that is authored by the same organization that authored the Reference Document (a.k.a. an “authoritative” Reference).

If I disagree with an Informative Reference assertion, can I provide feedback?

Please provide feedback regarding anything related to an Informative Reference to olir@nist.gov (https://www.nist.govmailto:olir@nist.gov).

How should Federal agencies use the Online Informative References?

Users often need to compare two cybersecurity or privacy documents for a variety of reasons, such as demonstrating where the documents’ cybersecurity controls are similar and where gaps exist. The Derived Relationship Mapping (DRM) Analysis Tool (https://csrc.nist.gov/Projects/Cybersecurity-Framework/Derived-Relationship-Mapping) provides users with a convenient way to quickly view how one document may relate to another by leveraging the Focal Document. When a User compares the relationships from different Reference Documents and infers additional relationships among them, those inferred—derived—relationships are non-authoritative. The DRM Analysis tool provides users with the ability to leverage expert assertions from Subject Matter Experts (SMEs) and represents a starting point when attempting to compare Reference Documents.

Another popular use case involves conducting a gap analysis between documents. An analyst could leverage the DRM Analysis Tool to identify significant changes between two versions of the same document. An analyst could also use the tool to identify the gaps that would need to be addressed if their organization adopted a new security framework by generating reports comparing the Reference Documents they already comply with to the Reference Document for the new security framework.

Communication with NIST

How can I ensure resources or case studies my organization has released publicly are visible for others to use?

Share them with NIST via email (cyberframework@nist.gov(link sends e-mail) (https://www.nist.govmailto:cyberframework@nist.gov)), sector organizations (where applicable), trade and professional associations, and post information on your organization's website.

Does NIST encourage translations of the Cybersecurity Framework? If so, is ther procedure to follow?

NIST's policy is to encourage translations of the Framework. After an independent check on translations, NIST typically will post links to an external website with the translation. These links appear on the Cybersecurity Framework's International Resources (https://www.nist.gov/cyberframework/international-resources) page.

Those wishing to prepare translations are encouraged to use the Cybersecurity Framework Version 1.1 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

Who can answer additional questions regarding the Framework?

Review the NIST Cybersecurity Framework web page for more information, contact NIST via email at cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov), and check with sector or relevant trade and professional associations.

How do I sign up for the mailing list to receive updates on the NIST Cybersecurity Framework?

To receive updates on the NIST Cybersecurity Framework, you will need to sign up for NIST E-mail alerts. The sign-up box is located at the bottom-right hand side on each Cybersecurity Framework-based web page, or on the left-hand side of other NIST pages. Once you enter your email address and select a password, you can then select "Cybersecurity Framework" under the "Subscription Topics" to begin receiving updates on the Framework. If you see any other topics or organizations that interest you, please feel free to select those as well. You may change your subscription settings or unsubscribe at anytime.

How can I share my thoughts or suggestions for improvements to the Cybersecurity Framework with NIST?

There are many ways to participate in Cybersecurity Framework.

Participation in NIST Workshops, RFI responses, and public comment periods for work products are excellent ways to inform NIST Cybersecurity Framework documents. Less formal but just as meaningful, as you have observations and thoughts for improvement, please send those to cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov). We value all contributions through these processes, and our work products are stronger as a result.

Participation in the larger Cybersecurity Framework ecosystem is also very important. NIST's vision is that various sectors, industries, and communities customize Cybersecurity Framework for their use. Customization efforts include:

- Financial Services Sector Cybersecurity Profile (https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile)
- cross-walking key legislation and regulation to the Cybersecurity Framework (e.g., Health and Human Services' HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf)),
- developing Profiles that reflect business/mission priorities of a given stakeholder group (e.g., Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC) Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf)),
- publishing case studies on Cybersecurity Framework implementation (e.g., The Cybersecurity Framework in Action: An Intel Use Case (https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf))
- sharing guidance and successful implementation through Success Stories (https://www.nist.gov/cyberframework/success-stories) (e.g. The University of Chicago's Biologic es Division (https://www.nist.gov/cyberframework/success-stories/stories) implementation)

If you develop similar resources, NIST is happy to consider them for inclusion in the Industry Resources page.

Thank you very much for your offer to help. Please keep us posted on your ideas and work products.

How can I engage with NIST relative to the Cybersecurity Framework?

NIST welcomes active participation and suggestions to inform the ongoing development and use of the Cybersecurity Framework.

Public and private sector stakeholders are encouraged to participate in NIST workshops and submit public comments to help improve the NIST Cybersecurity Framework and related guidelines and resources. Also, NIST is eager to hear from you about your successes with the Cybersecurity Framework and welcomes submissions for our Success Stories (https://www.nist.gov/cyberframework/success-stories), Risk Management Resources (https://www.nist.gov/cyberframework/resources/risk-management-resources), and Perspectives (https://www.nist.gov/cyberframework/perspectives) pages. Lastly, please send your observations and ideas for improving the CSFto cyberframework@nist.gov (https://www.nist.govmailto:cyberframework@nist.gov). We value all contributions, and our work products are stronger and more useful as a result!

To receive updates on the NIST Cybersecurity Framework, you may sign up for NIST email alerts via the Email Subscription (https://service.govdelivery.com/accounts/USNIST/subscriber/new) page. Once you enter your email address and select a password, you can then select "Cybersecurity Framework" under the "Subscription Topics" to begin receiving updates on the Framework. If you see any other topics or organizations that interest you, please feel free to select those as well. You may change your subscription settings or unsubscribe at any time.

Created February 13, 2018, Updated June 16, 2021